Proskauer

SEC Revisits Regulation S-P After Twenty Years of Innovation to Information Technology

April 4, 2023

On March 15, 2023, the U.S. Securities and Exchange Commission ("SEC") released its proposal to amend Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information (the "Proposed Amendments"), while simultaneously issuing two additional cybersecurity-related rule proposals[1] and re-opening the comment period for its previously proposed cybersecurity risk management rule released in February 2022.[2] This set of sweeping reforms makes it clear, if not already, that the SEC is serious about implementing comprehensive cybersecurity and privacy standards across its regulated entity population — including investment advisers. However, the Proposed Amendments are already subject to criticism, most notably by Commissioner Pierce in her accompanying Statement, [3] due to the likely burdens and costs of implementation, as well as the potential for conflicts with existing state laws. Moreover, the Proposed Amendments would create additional exam and enforcement risk where disclosure of certain cyber events is deemed – after the fact – not to have been prompt or accurate enough.

Background

Regulation S-P ("Reg. S-P") requires, among other things, covered firms to adopt written policies and procedures designed to protect the personally identifiable information of such firms' natural person customers contained in its records (the "Safeguards Rule"). Reg. S-P applies to SEC registered investment advisers, investment companies, broker dealers and transfer agents ("covered firms"); [4] it does not apply to unregistered advisers (e.g., exempt reporting advisers) or private funds relying on sections 3(c)(1) or 3(c)(7) under the Investment Company Act.[5] Reg S-P was adopted in 2000, before widespread use of mobile devices, remote work and the "cloud." In the early years following Reg. S-P's adoption, compliance efforts often amounted to adopting policies and procedures that were focused on the physical security of paper files containing covered customer information (e.g., by requiring the use of locked file cabinets). It has since evolved, however, into a framework for the protection and safeguarding of covered information largely stored electronically.

In recognition of the significant changes to business operations and the extensive reliance on (and vulnerabilities posed by) electronic storage and communications, the Proposed Amendments would amend the Safeguards Rule to enhance required procedures by mandating an incident response plan to address security breaches. The Proposed Amendments would also expand the scope of information and customers covered by these requirements. Additionally, if the Proposed Amendments are adopted, the privacy notice requirement of Reg. S-P would be simplified through the implement of a 2015 legislative change, which limits the need for annual delivery of the privacy notice in certain cases.

Adoption of an Incident Response Plan

The centerpiece of the Proposed Amendments is a new requirement for covered firms to adopt a written incident response program ("IRP") as part of its written Reg. S-P policies that is "reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information." IRPs would be required to provide for:

- Assessment of the scope and scale of a breach, including the systems, customers and information accessed or used without authorization;
- Steps to contain and control further unauthorized access or use; and
- Notification protocols for those customers whose "sensitive information" was, or was likely to have been, involved in the breach.

The Proposed Amendments would also require covered firms to enter into a written agreement with each service provider that requires the service provider to (i) take appropriate measures to safeguard customer information, and (ii) notify the covered firm in the event of unauthorized access to a customer information system maintained by the service provider (no later than 48 hours after becoming aware of the breach). This would encompass a very broad universe of service providers, including email, CRM system, cloud-based and other technology vendors. As noted by Commissioner Peirce, however, renegotiating existing contracts with service providers may prove to be expensive and time consuming and may not be feasible in all cases.[6]

Establishing a Federal Minimum Standard for Notification of an Information Breach

Covered firms are currently subject to a patchwork of state privacy laws across all 50 states, ranging in degree of compliance burden depending on where they and their clients or investors are located. The SEC intends to create a federal minimum standard for notification requirements of covered firms that experience an information breach. Such notification would be required where the information breach is likely to result in "sensitive customer information"[7] being used in a manner that would result in substantial harm or inconvenience. The Proposed Amendments call for the notification:

- To be made to each affected individual or, if the specific individual(s) is not ascertainable, all individuals for which the covered firm possesses sensitive customer information;
- To be made within 30 days of becoming aware of such unauthorized access or use (with a limited 30-day extension for matters of national security);[8]
- To include the following: (i) a description of the incident in general terms and information to have been accessed or used, (ii) a description of any remedial action and preventative measures, (iii) the date or estimated date of the incident, (iv) a point of contact at the covered firm for the individual to inquire into the matter, (v) a recommendation for the individual to review their account statements (if applicable), (vi) an explanation of what a fraud alert is and information to assist the individual in establishing a fraud alert in their credit report, (vii) a recommendation that the individual periodically obtain and review a credit report and have any fraudulent transaction deleted, (viii) an explanation of how the individual may obtain a free credit report, (ix) instructions on how to obtain additional online guidance from the Federal Trade Commission ("FTC") and usa.gov, and (x) a statement encouraging the individual to report incidents of identity theft to the

FTC.

While the Proposed Amendments are intended to establish a minimum set of standards that would be consistent with (or at least more stringent than) applicable state laws, and while the SEC appears to have extensively reviewed state privacy laws in connection with these proposals, the SEC has nevertheless requested comments as to whether the Proposed Amendments would conflict with any specific state laws.[9]

Annual Privacy Notice Requirements

Reg. S-P requires covered firms to deliver an annual privacy notice to its customers. The Proposed Amendments would implement a 2015 legislative change, which created an exception to the annual privacy notice requirements where the covered firm's policies and practices regarding customer information are unchanged.

Intersection with the SEC's Investment Management Cybersecurity Proposal

There is significant overlap between the Proposed Amendments and the SEC's Cybersecurity Proposal issued in February 2022, applicable to registered investment advisers and other regulated entities, which is summarized in our previous Client Alert. The Cybersecurity Proposal requires the adoption of a cybersecurity incident response program, which is similar to the incident response plan called for by the Proposed Amendments. Additionally, the Cybersecurity Proposal creates an obligation to report "significant cybersecurity incidents" to the SEC. Under the Proposed Amendments, an information breach that triggers mandatory customer notification (within 30 days), would also amount to a significant cybersecurity incident that triggers an SEC reporting requirement (within 48 hours). The SEC acknowledges this overlap in the Proposed Amendments and offers assurances that entities required to comply with both rules, if adopted, would be able to avoid duplicative efforts by adopting one set of policies or providing a single notice, where applicable.

Intersection with the SEC's Examination and Enforcement Efforts

The SEC has long been focused on the risks that cybersecurity incidents pose to covered firms and, by extension, to their investors, clients and customers. That focus extends beyond rulemaking and includes significant devotion of resources to examination and enforcement. The Division of Examinations has made information security and resilience an examination priority every year since 2014, and it did so again in 2023.[10] Similarly, the Division of Enforcement has repeatedly brought enforcement actions in this area, including fourteen relating to cybersecurity controls and safeguarding customer information since 2015,[11] pursuing these actions through its dedicated Crypto Assets and Cyber Unit which recently almost doubled in size to fifty professionals.[12] In addition to pursuing violations uncovered during the course of routine compliance examinations, the Examinations and Enforcement Divisions also proactively investigate potential violations of which they become aware, either through whistleblowers or public news reports of prominent security breaches, such as the late 2020 SolarWinds cyber breach.[13] SEC examination and enforcement focus in this area can therefore be expected to continue — and possibly even increase — creating more risk for firms as compliance obligations expand.

Timing and Applicability

Comments are due within 60 days after the Proposed Amendments are published in the Federal Register, which coincides with the re-opening of the comment period for the Cybersecurity Proposal. There would be a 12-month transition period if the Proposed Amendments were to be adopted.

Please contact one of our Private Funds Group or Privacy & Cybersecurity partners for more information.

---

[1] Cybersecurity Risk Management Proposed Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, Exchange Act Release No. 34-97142 (Mar. 15, 2023) ("Exchange Act Cybersecurity Proposal"), and Regulation Systems Compliance and Integrity, Exchange Act Rel. No. 34-97143 (Mar. 15, 2023) ("Regulation SCI Proposal").

[2] Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Securities Act Rel. No. 11028 (Feb. 9, 2022) ("Cybersecurity Proposal").

[3] Commissioner Hester M. Peirce, Statement on Regulation SP: Privacy of Consumer Financial Information and Safeguarding Customer Information, March 15, 2023 ("Pierce Statement").

[4] The Proposed Amendments define "covered institution" as "any broker or dealer, any investment company and any investment adviser or transfer agent registered with the Commission or another appropriate regulatory agency ("ARA") as defined in Section 3(a)(34)(B) of the Securities Exchange Act of 1934." Rule 248.30(e)(3).

[5] Exempt reporting advisers and private funds are subject to the Consumer Financial Protection Bureau's Regulation P, 12 CFR Part 1016, and the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR Part 314.

[6] Pierce Statement ("How much will it cost to renegotiate all of those contracts? Will it even be possible to do so? What happens to a covered institution whose service provider chooses not to play ball?").

[7] The Proposed Amendments add the new term "sensitive customer information," and defines it as customer information that could create a substantial harm or inconvenience in the event of an information breach. Sensitive customer information would include, for example, a customer's: social security number; official State or government issued driver's license or identification number; alien registration number; government passport number; employer or taxpayer identification number; a biometric record; a unique electronic identification number; address; or routing code.

[8] Notably, the Proposed Amendments do not provide for exceptions where delay is needed for other law enforcement-related reasons beyond national security. However, the SEC has requested comments as to whether to include such exceptions. Proposed Amendments, request for comment 56 at p. 63. See also Pierce Statement ("While I support customer notification, the rule should include a law enforcement exception permitting covered institutions to delay alerting customers about an unauthorized incursion when there is a valid law enforcement or national security need for doing so. We are making the small concession of allowing the Attorney General to obtain a delay of up to 30 days, if he can cite a substantial risk to national security in writing.").

[9] Proposed Amendments, request for comment 34 at p. 46. See also Pierce Statement ("What is a firm that finds itself pinched between competing state and federal notification rules supposed to do? Rather than preempting or deferring to state law, we dance around the problem we are creating and provide no workable strategy for firms to manage the conflict.").

[10] SEC Division of Examinations, 2023 Examination Priorities, at pp. 13-14.

[11] SEC Website, Crypto Assets and Cyber Enforcement Actions — Regulated Entities – Cybersecurity Controls and Safeguarding Customer Information.

[12] SEC Press Release, SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit, May 3, 2022.

[13] Reuters, U.S. SEC probing SolarWinds clients over cyber breach disclosures -sources, June 22, 2021.

Related Professionals

- **Nolan M. Goldberg**
  Partner
- **Robert Pommer**
  Partner
- **Robert H. Sutton**
  Partner